8e6 Technologies

8e6 Threat Analysis Reporter

QUICK START GUIDE

Model: TAR 1.0

TAR "S" (5K02-62), TAR "H" (5K02-66), TAR "MSA" (5K02-67)

Release 1.1.00 / Version No.: 06.18.07

Downloaded from www.Manualslib.com manuals search engine

8e6 Threat Analysis Reporter Quick Start Guide

© 2007 8e6 Technologies. All rights reserved.

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form without prior written consent from 8e6 Technologies.

Every effort has been made to ensure the accuracy of this document. However, 8e6 Technologies makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. 8e6 Technologies shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Trademarks

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Part# TAR-QSG-070618

Downloaded from www.Manualslib.com manuals search engine

Contents

Threat Analysis Reporter Introduction 1

About this Document 2

Conventions Used in this Document 2

Service Information 3

Preliminary Setup Procedures 4

Unpack the Unit from the Carton 4

Rack Mount the “S” or “MSA” Server 5

Install the “H” Server Bezel 8

Rack Mount the “H” Server 11

Install the Server 14

Step 1: Initial Setup Procedures 14

Step 2: Physically Connect the Unit to the Network 29

Step 3: Wizard Setup Procedures 30

Conclusion 42

Specifications 43

Physical Specifications 43

Internal Product Specifications 43

Hardware Component Specifications 44

“S” and “MSA” Front Panel LED Indicators, Buttons 45

Appendix: Optional Ethernet Tap Installation 46

Preliminary Setup Procedures 46

Install the Ethernet Tap Unit 47

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Threat Analysis Reporter Introduction

Thank you for choosing to evaluate the 8e6 Technologies Threat Analysis Reporter. This product addresses user-generated Web threats such as excessive use of bandwidth and inappropriate Internet usage, and provides network administrators tools to monitor such threats so management can enforce corporate Internet usage policies.

Working in conjunction with 8e6's R3000 Enterprise Filter, the Threat Analysis Reporter translates end user Internet activity from the R3000's logs into dynamic graphical snapshots of network Internet traffic. Using remediation tools in the console, administrators and management can then manage and control user-generated Web threats in real time.

Downloaded from www.Manualslib.com manuals search engine

About this Document

This document is divided into the following sections:

- **Introduction** - This section is comprised of an overview of the Threat Analysis Reporter product and how to use this document
- **Service Information** - This section provides 8e6 Technologies contact information
- **Preliminary Setup Procedures** - This section includes instructions on how to physically set up the Threat Analysis Reporter unit in your network environment
- **Install the Server** - This section explains how to configure the Threat Analysis Reporter
- **Conclusion** - This section indicates that the quick start steps have been completed
- **Specifications** - This section features hardware specifications and descriptions of front panel LED indicators
- **Appendix: Optional Ethernet Tap Installation** - This appendix explains how to install the optional Ethernet Tap device on your network for bandwidth monitoring if you have a TAR “S” or TAR “H” server

Conventions Used in this Document

The following icons are used throughout this document to call attention to important information pertaining to handling, operation, and maintenance of the server; safety and preservation of the equipment, and personal safety:

NOTE: *The “note” icon is followed by additional information to be considered.*

WARNING: *The “warning” icon is followed by information alerting you to a potential situation that may cause damage to property or equipment.*

Downloaded from www.Manualslib.com manuals search engine

Service Information

The user should not attempt any maintenance or service on the unit beyond the procedures outlined in this document.

Any initial hardware setup problem that cannot be resolved at your internal organization should be referred to an 8e6 Technologies solutions engineer or technical support representative.

8e6 Corporate Headquarters (USA)

Local	:	714.282.6111
Domestic US	:	1.888.786.7999
International	:	+1.714.282.6111

8e6 Taiwan

Taipei Local	:	2501-5285
Domestic Taiwan	:	02-2501-5285
International	:	886-2-2501-5285

Procedures

When calling 8e6 Technologies regarding a problem, please provide the representative the following information:

- Your contact information.
- Serial number or original order number.
- Description of the problem.
- Network environment in which the unit is used.
- State of the unit before the problem occurred.
- Frequency and repeatability of the problem.
- Can the product continue to operate with this problem?
- Can you identify anything that may have caused the problem?

Downloaded from www.Manualslib.com manuals search engine

Preliminary Setup Procedures

Unpack the Unit from the Carton

Inspect the packaging container for evidence of mishandling during transit. If the packaging container is damaged, photograph it for reference.

Carefully unpack the unit from the carton and verify that all accessories are included. Save all packing materials in the event that the unit needs to be returned to 8e6 Technologies.

The carton should contain the following items:

- 1 Threat Analysis Reporter unit
- 1 AC Power Cord
- 1 Serial Port Cable
- 1 CAT-5E Crossover Cable
- 1 CAT-5E Coupler
- Rack Mount Brackets (2)
- 1 End User License Agreement (EULA)
- 1 envelope containing a CD-ROM with a PDF of the Threat Analysis Reporter User Guide. The latest version of the user guide can be obtained from our Web site at **http://www.8e6.com/docs/tar_ug.pdf**.

NOTE: *TAR "S" and "H" units come with a NetOptics 10/100BaseT Ethernet Tap kit to be installed at your option. TAR "H" units also come with a separate bezel to be installed on the front of the chassis, and an additional AC power cord.*

Inspect the server and accessories for damage. If the contents appear damaged, file a damage claim with the carrier immediately.

For "S" and "MSA" units, proceed to the instructions for Rack Mount the "S" or "MSA" Server.

For "H" units, proceed to the instructions for Install the "H" Server Bezel, followed by Rack Mount the "H" Server.

Downloaded from www.Manualslib.com manuals search engine

Rack Mount the “S” or “MSA” Server

Rack Mount Instructions

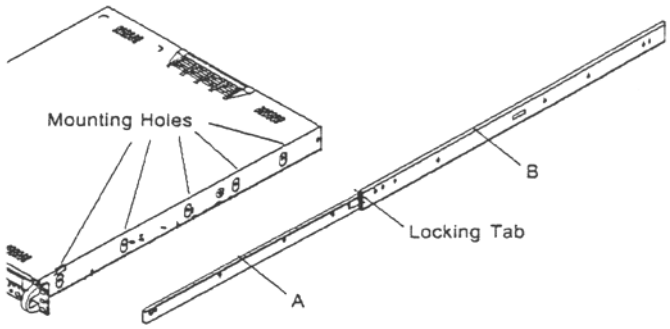
Rack Setup Suggestions

- Determine the placement of each component in the rack before you install the rails.
- Install the heaviest server components on the bottom of the rack first, and then work up.

Identify the Sections of the Rack Rails

You should have received two rack rail assemblies with the 8e6 server unit. Each of these assemblies consists of two sections: An inner fixed chassis rail that secures to the unit (A), and an outer fixed rack rail that secures directly to the rack itself (B). A sliding rail guide sandwiched between the two should remain attached to the fixed rack rail. The A and B rails must be detached from each other in order to install.

To remove the fixed chassis rail (A), pull it out as far as possible. You should hear a “click” sound as a locking tab emerges from inside the rail assembly and locks the inner rail. Then depress the locking tab to pull the inner rail completely out. Do this for both the left and right side rack rail.



Install the Chassis Rails

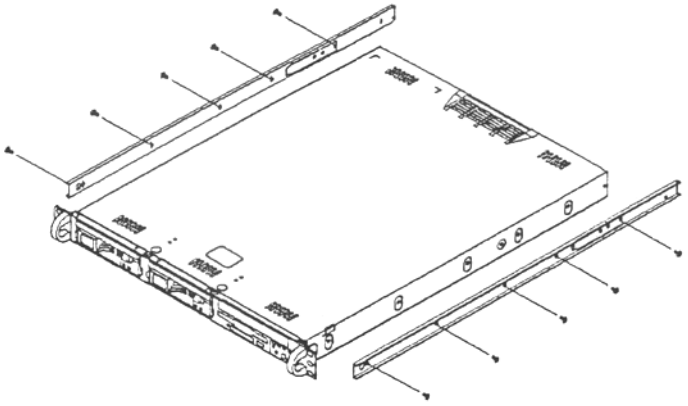
Position the fixed chassis rail sections you just removed along the side of the server chassis making sure the five screw holes line up. Note that these two rails are left/right specific. Screw the rail securely to the side of the chassis. Repeat this procedure for the other rail on the other side of the chassis. You will also need to attach the rail brackets when installing into a Telco rack.

Locking Tabs: As you have seen, both chassis rails have a locking tab, which serves two functions. The first is to lock the server into place when installed and pushed fully into the rack, which is its normal position. Secondly, these tabs also lock the server in place when fully extended from the rack. This prevents the server from coming completely out of the rack when you pull it out for servicing.

Downloaded from www.Manualslib.com manuals search engine

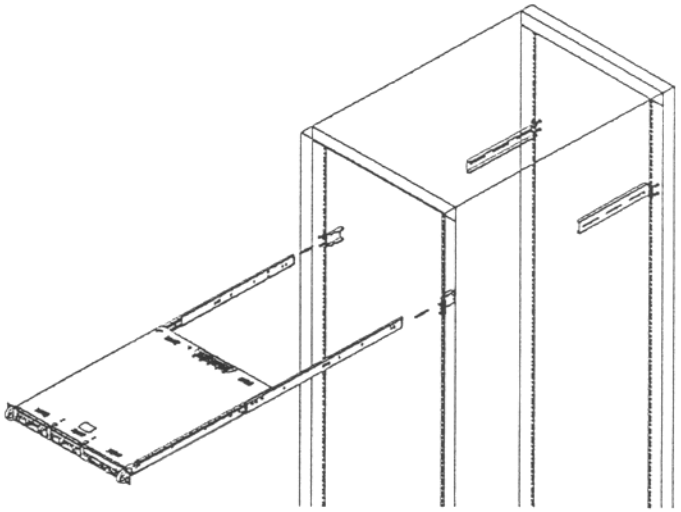
Install the Rack Rails

Determine where you want to place the server unit in the rack. Position the fixed rack rail/sliding rail guide assemblies at the desired location in the rack, keeping the sliding rail guide facing the inside of the rack. Screw the assembly securely to the rack using the brackets provided. Attach the other assembly to the other side of the rack, making sure that both are at the exact same height and with the rail guides facing inward.



Install the Server into the Rack

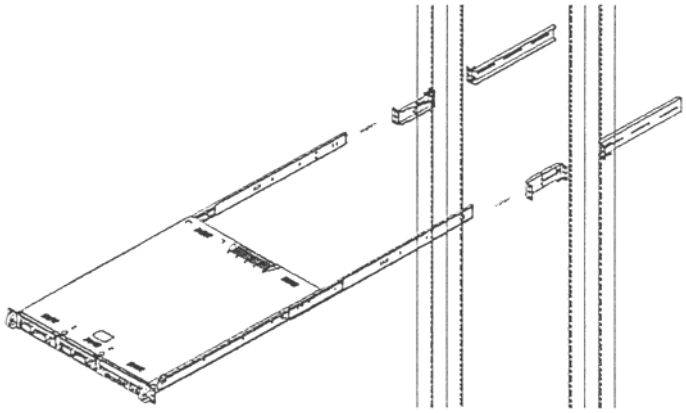
You should now have rails attached to both the chassis and the rack unit. The next step is to install the server chassis into the rack. Do this by lining up the rear of the chassis rails with the front of the rack rails. Slide the chassis rails into the rack rails, keeping the pressure even on both sides (you may have to depress the locking tabs when inserting).



Downloaded from www.Manualslib.com manuals search engine

Installing the Server into a Telco Rack

If you are installing the 8e6 server unit into a Telco type rack, follow the directions given on the previous pages for rack installation. The only difference in the installation procedure will be the positioning of the rack brackets to the rack. They should be spaced apart just enough to accommodate the width of the Telco rack.



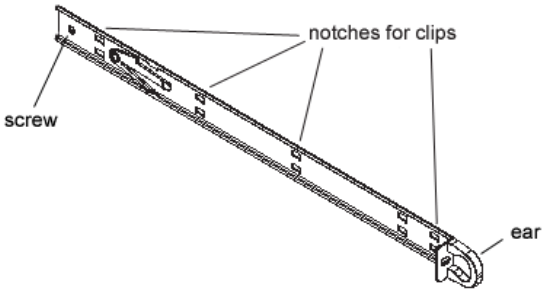
Downloaded from www.Manualslib.com manuals search engine

Install the “H” Server Bezel

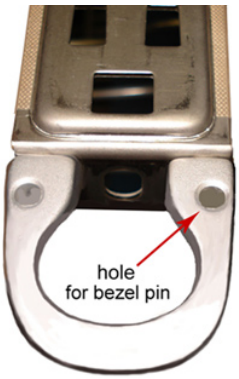
Before rack mounting the “H” unit, the bezel should be installed on the front end of the chassis. This portion of the installation process requires you to unpack the unit and bezel.

NOTE: *The bezel has been packaged separately from the unit to prevent damage during shipping.*

Front of bezel

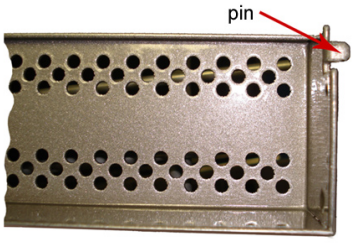


Outside of left inner rail



Inside front end of left inner rail

Inner left rail attached to chassis

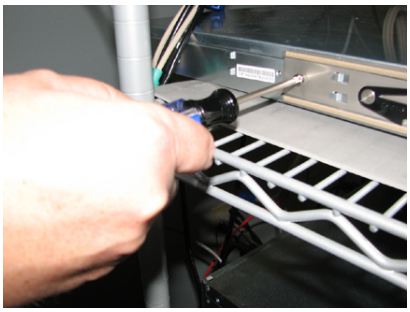


Pin on right side of bezel

Downloaded from www.Manualslib.com manuals search engine

A. Remove the plastic wrapping from the left and right ears.

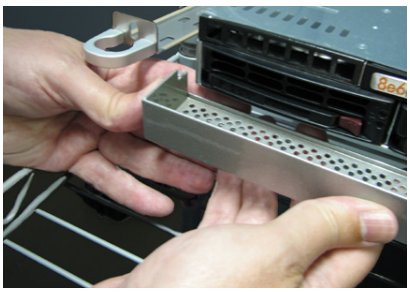
B. On one side of the chassis (left or right), unscrew the inner rail from the chassis.



C. Slide the loosened inner rail slightly backwards to release it from the clips at the side of the chassis, and then lay it down beside the chassis, with the inside of the rail facing up.

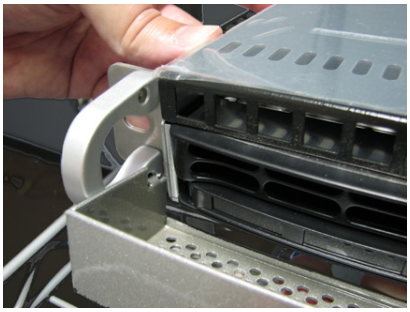
D. On the inner rail that is still attached to the chassis, insert the bezel pin into the bottom hole of the ear. Be sure the pin is pushed all the way in so that it is flush against the ear.

E. Take up the free end of the bezel and also the loosened inner rail.



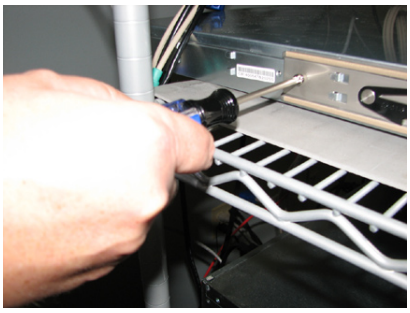
Downloaded from www.Manualslib.com manuals search engine

F. Return the loosened inner rail to its upright position and insert the bezel pin into the bottom hole of the ear.



G. Slide the inner rail forward beneath the clips to lock it in place.

H. Screw the inner rail back on the chassis.



I. After it is installed, the bezel should drop down when it is gently tugged forward and downward. The bezel should remain upright when raised up and closed.

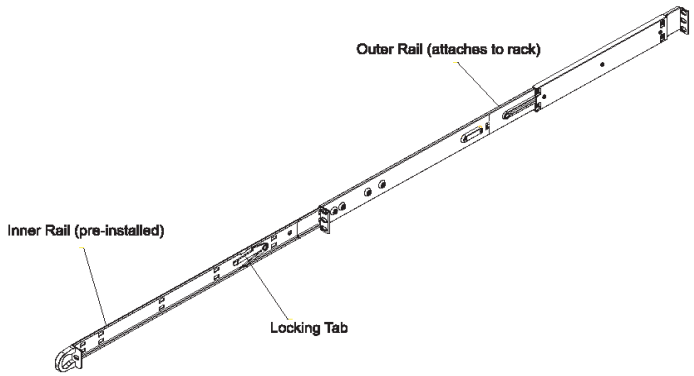
Downloaded from www.Manualslib.com manuals search engine

Rack Mount the “H” Server

Rack Mount Instructions

Identify the Sections of the Rack Rails

You should have received two rack rail assemblies with the 8e6 server unit. Each of these assemblies consists of two sections: An inner fixed chassis rail that secures to the unit (A), and an outer fixed rack rail that secures directly to the rack itself (B). Two pairs of short brackets to be used on the front side of the outer rails are also included.



Install the Inner Rails

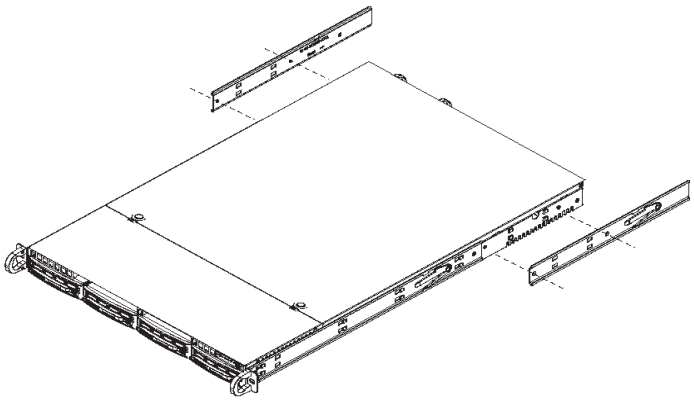
Both the left and right side inner rails have been pre-attached to the chassis. Proceed to the next step.

Install the Outer Rails

Begin by measuring the distance from the front rail to the rear rail of the rack. Attach a short bracket to the front side of the right outer rail and a long bracket to the rear side of the right outer rail. Adjust both the short and long brackets to the proper distance so that the rail can fit snugly into the rack. Secure the short bracket to the front side of the outer rail with two M4 screws and the long bracket to the rear side of the outer rail with three M4 screws. Repeat these steps for the left outer rail.

Locking Tabs: Both chassis rails have a locking tab, which serves two functions. The first is to lock the server into place when installed and pushed fully into the rack, which is its normal position. Secondly, these tabs also lock the server in place when fully extended from the rack. This prevents the server from coming completely out of the rack when you pull it out for servicing.

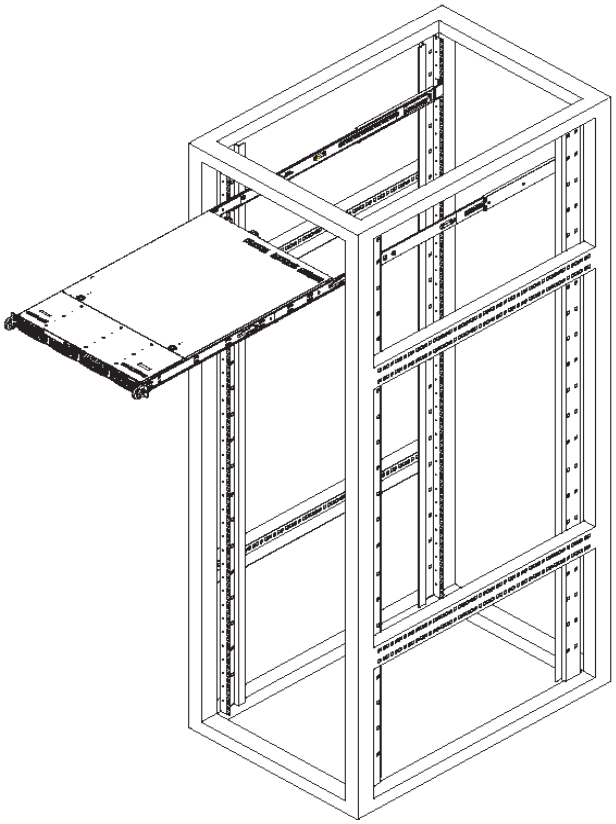
Downloaded from www.Manualslib.com manuals search engine



Install the Server into the Rack

You should now have rails attached to both the chassis and the rack unit. The next step is to install the server chassis into the rack. Do this by lining up the rear of the chassis rails with the front of the rack rails. Slide the chassis rails into the rack rails, keeping the pressure even on both sides (you may have to depress the locking tabs when inserting).

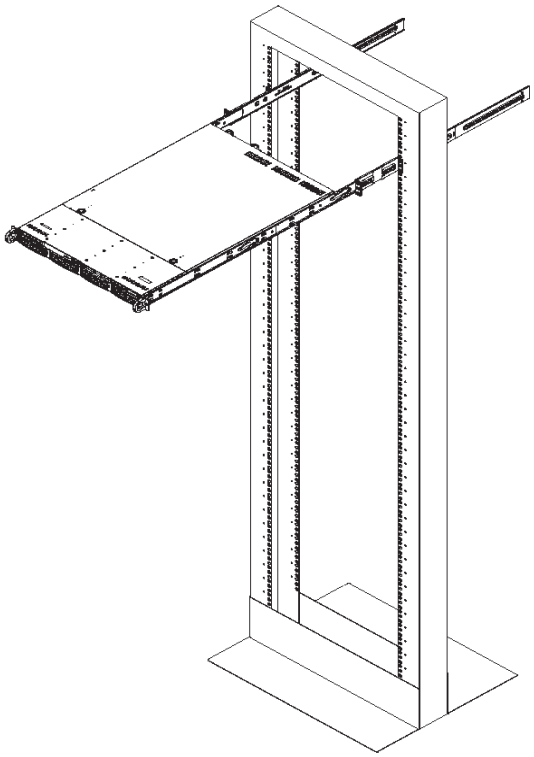
When the server has been pushed completely into the rack, you should hear the locking tabs “click.” Finish by inserting and tightening the thumbscrews that hold the front of the server to the rack.



Downloaded from www.Manualslib.com manuals search engine

Installing the Server into a Telco Rack

If you are installing the 8e6 server unit into a Telco type rack, follow the directions given on the previous page for rack installation. The only difference in the installation procedure will be the positioning of the rack brackets to the rack. They should be spaced apart just enough to accommodate the width of the Telco rack.



Downloaded from www.Manualslib.com manuals search engine

INSTALL THE SERVER

Step 1: Initial Setup Procedures

This step requires you to link the workstation to the Threat Analysis Reporter. The following hardware can be used for the initial setup procedures:

- Threat Analysis Reporter unit with AC power cord
- either one of two options:
  - PC monitor with AC power cord and keyboard, or
  - PC laptop computer with HyperTerminal and serial port cable (and USB DB9 serial adapter, if there is no serial port on your laptop)

NOTE: *Before installing the Threat Analysis Reporter server, the R3000 server to be used with this server must already be installed and running software version 1.10.15 or higher.*

Downloaded from www.Manualslib.com manuals search engine

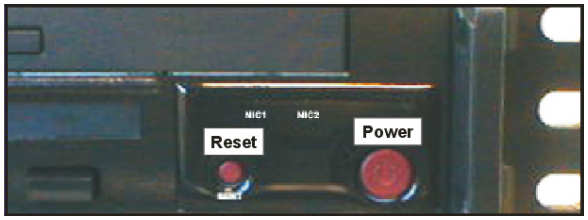
Link the Workstation to the Threat Analysis Reporter

Monitor and Keyboard Setup

A. Connect the PC monitor and keyboard cables to the rear of the chassis.

B. Turn on the PC monitor.

C. Power on the Threat Analysis Reporter unit by dropping down the face plate and pressing the large button at the right of the front panel (see image below).



Front of the chassis

Once the Threat Analysis Reporter is powered up, proceed to the Step-by-Step Initial Setup Procedures.

Serial Console Setup

A. Using the serial port cable (and USB DB9 serial adapter, if necessary), connect the laptop to the rear of the chassis (see images below).

Rear of the "S" or "MSA" chassis

Rear of the "H" chassis

B. Power on the laptop.

C. Power on the Threat Analysis Reporter by dropping down the face plate and pressing the large button at the right of the front panel (see top image on this page).

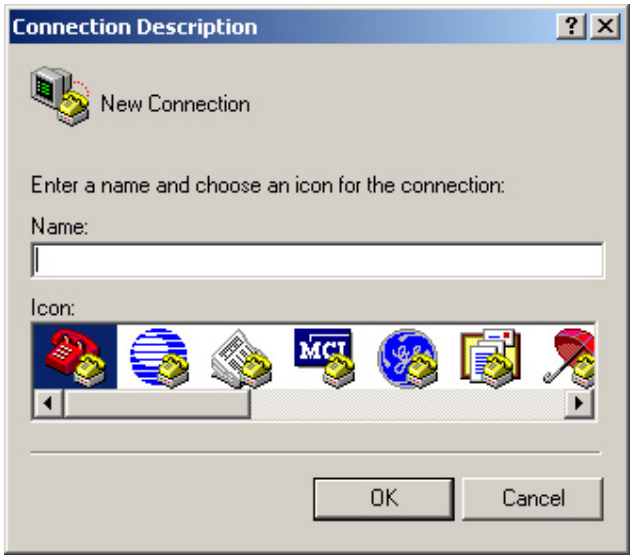
Once the Threat Analysis Reporter is powered up, proceed to the instructions for Hyper-Terminal Setup Procedures.

Downloaded from www.Manualslib.com manuals search engine

HyperTerminal Setup Procedures

If using a serial console, follow these procedures to create a HyperTerminal session.

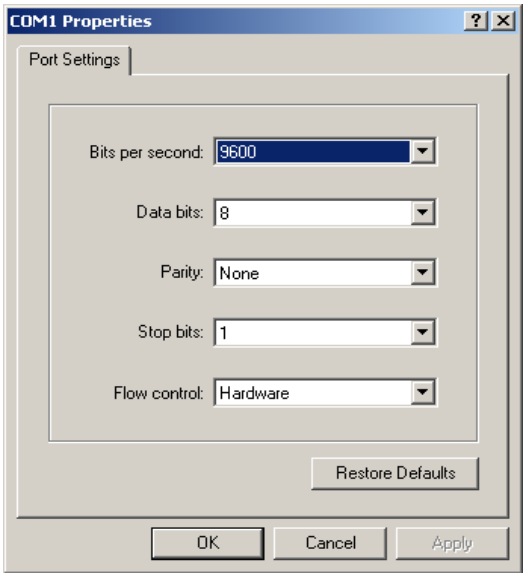
A. Launch HyperTerminal by going to Start > Programs > Accessories > Communications > HyperTerminal:



B. In the Connection Description dialog box, enter any session **Name**, and then click **OK** to open the Connect To dialog box:

Downloaded from www.Manualslib.com manuals search engine

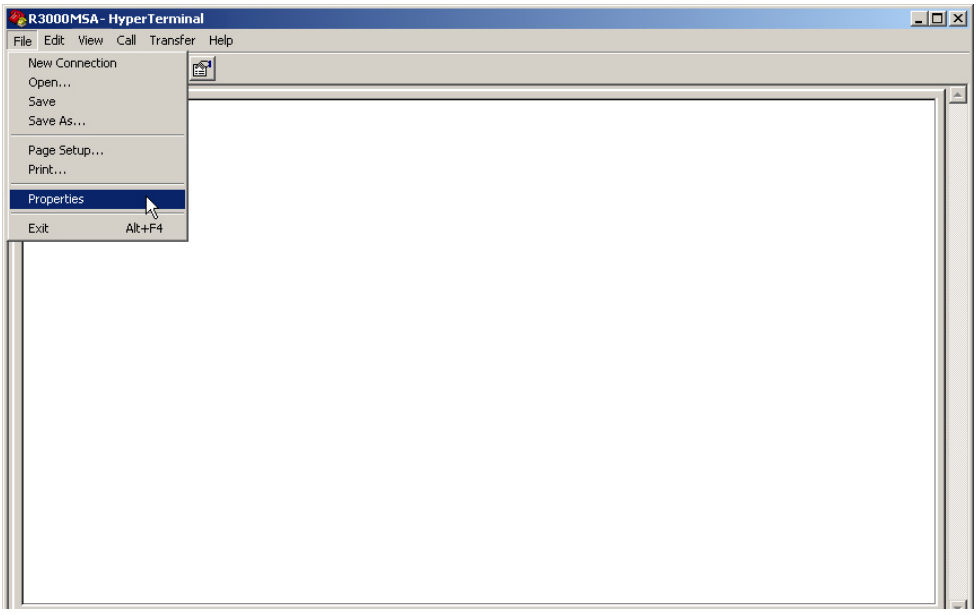
C. At the **Connect using** field, select the COM port assigned to the serial port on the laptop (probably “COM1”), and then click **OK** to open the Properties dialog box, displaying the Port Settings tab:



D. Specify the following session settings:

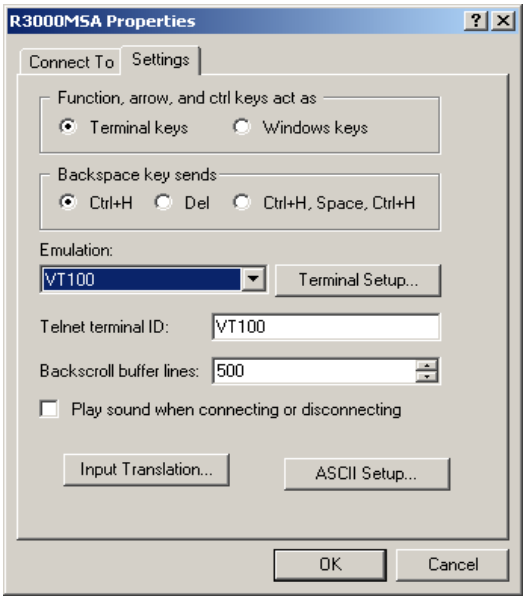
- Bits per second: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: Hardware

E. Click **OK** to connect to the HyperTerminal session:



Downloaded from www.Manualslib.com manuals search engine

F. In the HyperTerminal session window, go to File > Properties to open the Properties dialog box, displaying the Connect To and Settings tabs:



G. Click the Settings tab, and at the **Emulation** menu select “VT100”.

H. Click **OK** to close the dialog box, and to go to the login screen.

NOTE: *If using a HyperTerminal session, the login screen will display with black text on a white background.*

Downloaded from www.Manualslib.com manuals search engine

Step-by-Step Initial Setup Procedures

For these step-by-step procedures, you will need your network administrator to provide you the LAN 1 (Ethernet 0) and LAN 2 (Ethernet 1) IP address and subnet mask, gateway IP address, DNS server IP address(es), host name of the server, and IP address for the Web interface (if using a NAT device).

Login screen, password prompts

The login screen displays after powering on the Threat Analysis Reporter unit using a monitor and keyboard, or after creating a HyperTerminal session.

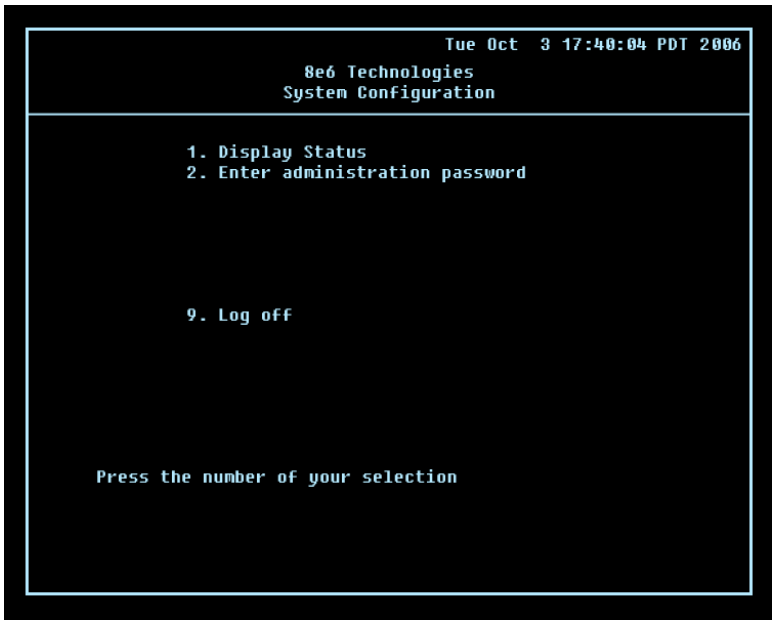
NOTE: *If the screensaver currently displays on your screen, press the* ***Enter*** *key to display the login screen.*

A. At the **login** prompt, type in ***menu***.

B. Press the **Enter** key to display the Password prompt.

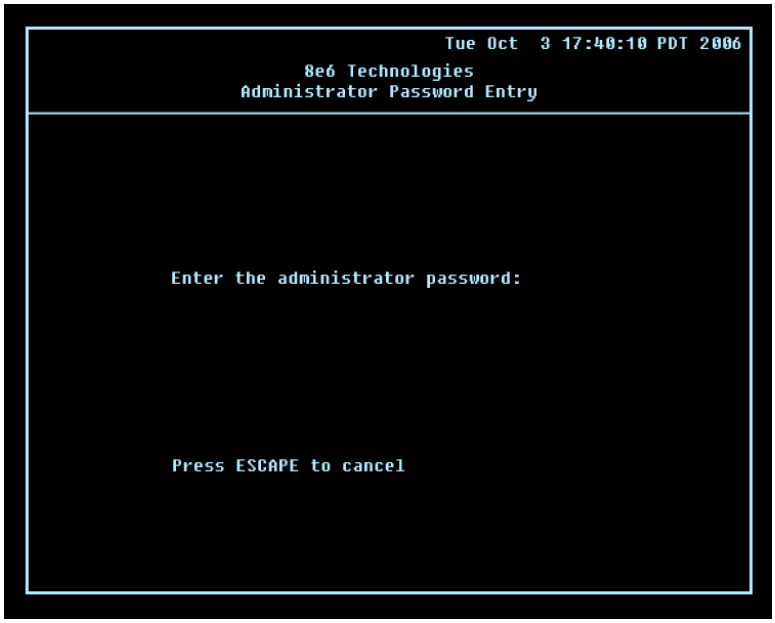
C. At the **Password** prompt, type in the following: ***#s3tup#r3k***

D. Press **Enter** to display the System Configuration screen:



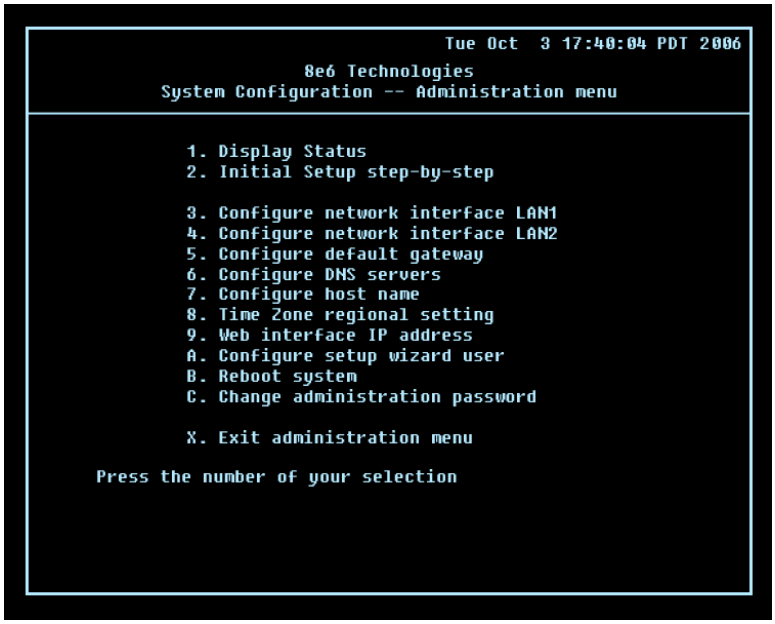
Downloaded from www.Manualslib.com manuals search engine

E. At the **Press the number of your selection** prompt, press **2** to display the Administrator Password Entry screen:



F. At the **Enter the administrator password** prompt, re-enter your password: ***#s3tup#r3k***

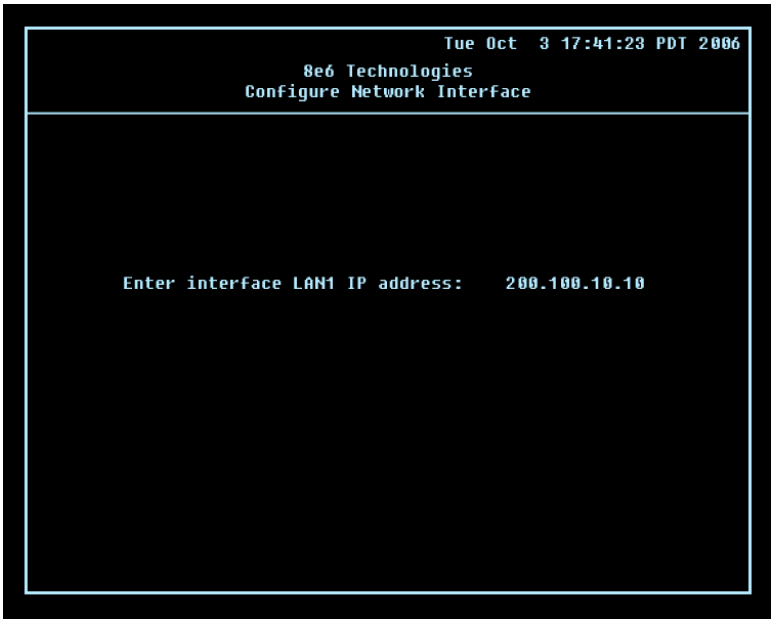
G. Press **Enter** to display the Administration menu where you can begin the step-by-step initial setup process using the configuration screens:


Tue Oct 3 17:40:04 PDT 2006
8e6 Technologies
System Configuration -- Administration menu
1. Display Status
2. Initial Setup step-by-step
3. Configure network interface LAN1
4. Configure network interface LAN2
5. Configure default gateway
6. Configure DNS servers
7. Configure host name
8. Time Zone regional setting
9. Web interface IP address
A. Configure setup wizard user
B. Reboot system
C. Change administration password
X. Exit administration menu
Press the number of your selection

H. At the **Press the number of your selection** prompt, press **2** to select the “Initial Setup step-by-step” process. This process takes you to the Configure Network Interface screen.

Downloaded from www.Manualslib.com manuals search engine

Configure Network Interface screen

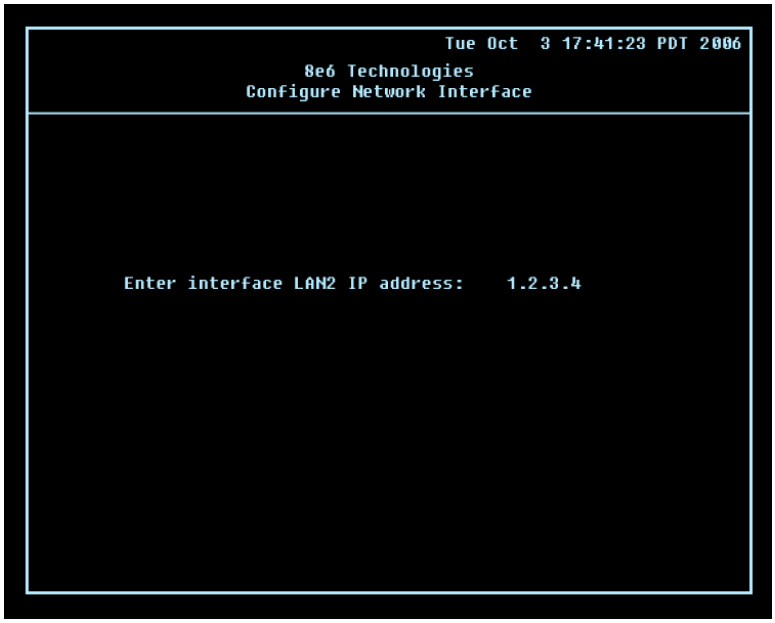


A. At the **Enter interface LAN1 (eth0) IP address** field, enter the IP address for the LAN 1 (Ethernet 0) interface, and then press **Enter** to go to the next screen.

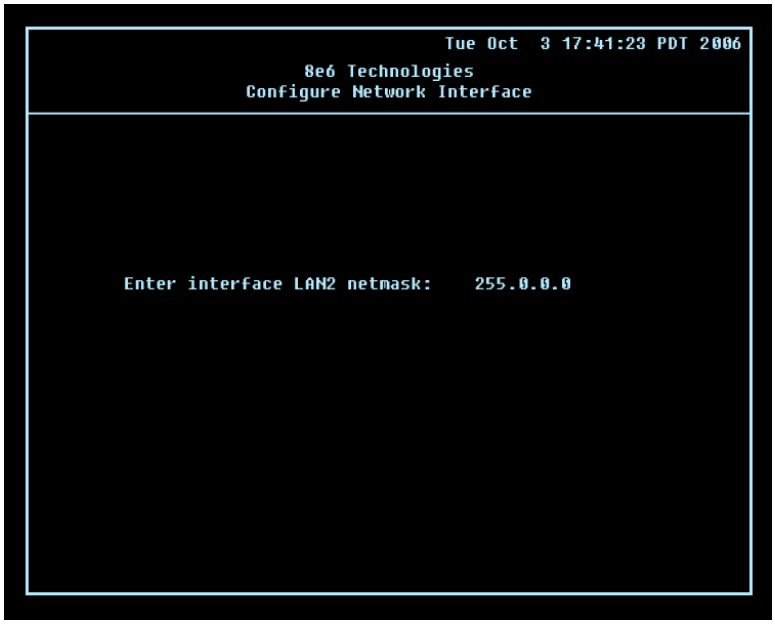
B. At the **Enter interface LAN1 (eth0) netmask** field, enter the subnet mask for the LAN 1 (Ethernet 0) interface using the dotted decimals notation format. Press **Enter** to display the confirmation prompt.

Downloaded from www.Manualslib.com manuals search engine

C. Press **Y** for “Yes” to confirm and save your entries for the LAN1 (eth0) interface, and to go to the next screen.



D. At the **Enter interface LAN2 (eth1) IP address** field, enter the IP address for the LAN 2 (Ethernet 1) interface, and then press **Enter** to go to the next screen.



E. At the **Enter interface LAN2 (eth1) netmask** field, using the dotted decimals notation format, enter the subnet mask for the LAN 2 (Ethernet 1) interface. Press **Enter** to display the confirmation prompt.

F. Press **Y** for “Yes” to confirm and save your entries for the eth1 interface, and to go to the Configure default gateway screen.

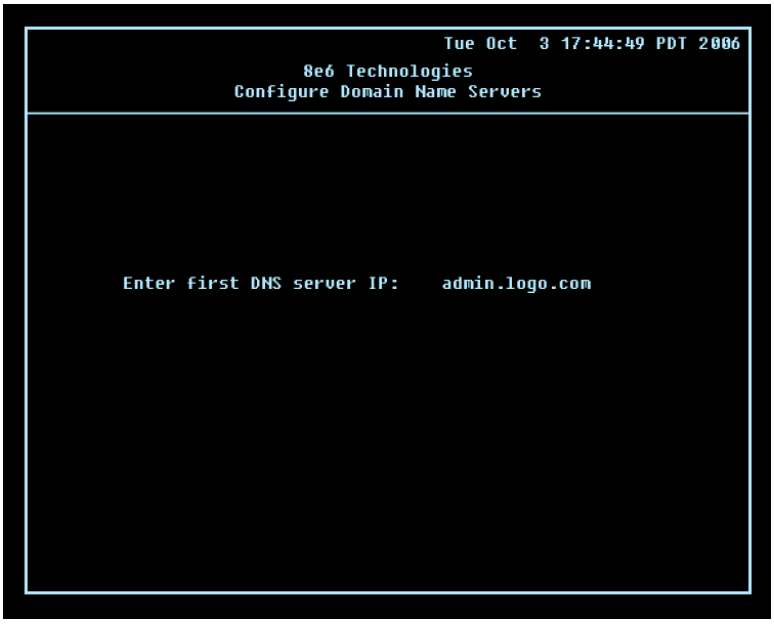
Downloaded from www.Manualslib.com manuals search engine

Configure default gateway screen

A. At the **Enter default gateway IP** field, enter the IP address for the default gateway. Press **Enter** to display the confirmation prompt.

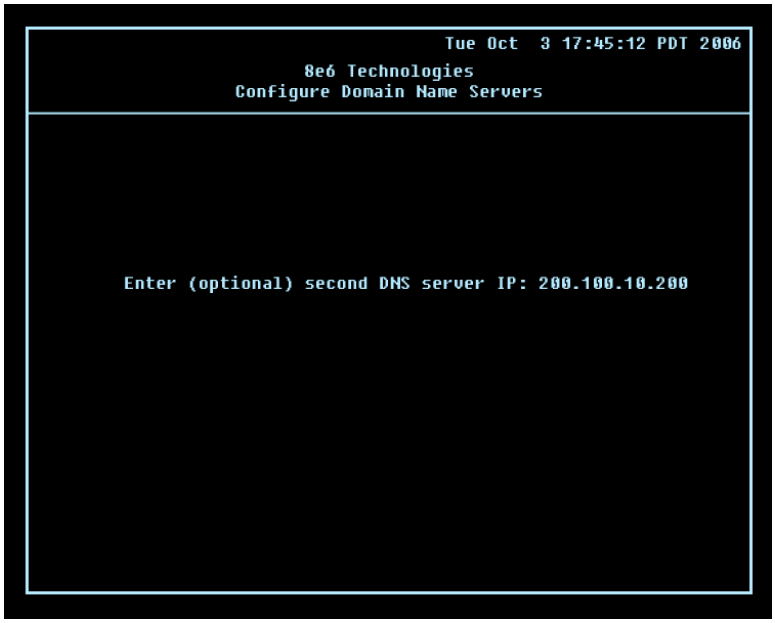
B. Press **Y** for “Yes” to confirm and save your entry for the gateway IP address, and to go to the Configure Domain Name Servers screen.

Configure Domain Name Servers screen



Downloaded from www.Manualslib.com manuals search engine

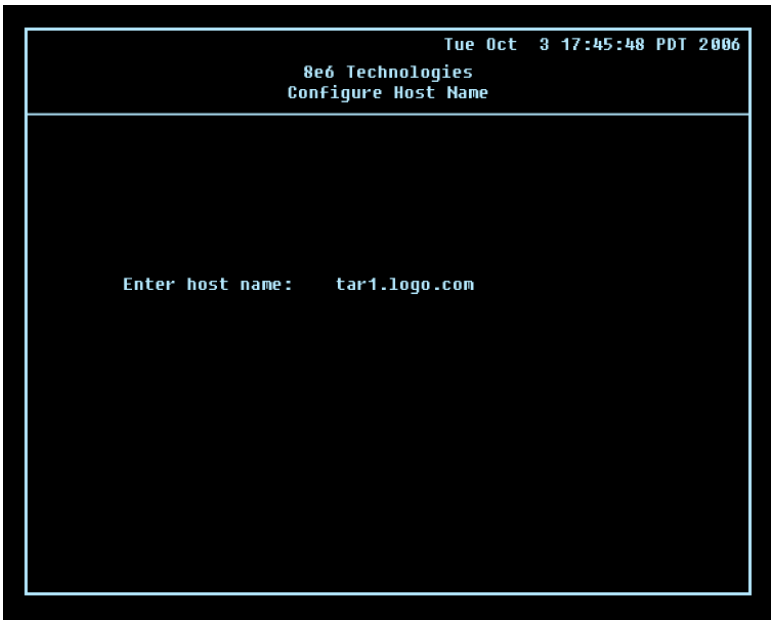
A. At the **Enter first DNS server IP** field, enter the IP address for the primary Domain Name Server. Press **Enter** to go to the next screen.


Tue Oct 3 17:45:12 PDT 2006
8e6 Technologies
Configure Domain Name Servers
Enter (optional) second DNS server IP: 200.100.10.200

B. At the **Enter (optional) second DNS server IP** field, if you have a secondary Domain Name Server you wish to use, enter the IP address for that server. Press **Enter** to display the confirmation prompt.

C. Press **Y** for “Yes” to confirm and save your entries for the domain name servers, and to go to the Configure Host Name screen.

Configure Host Name screen

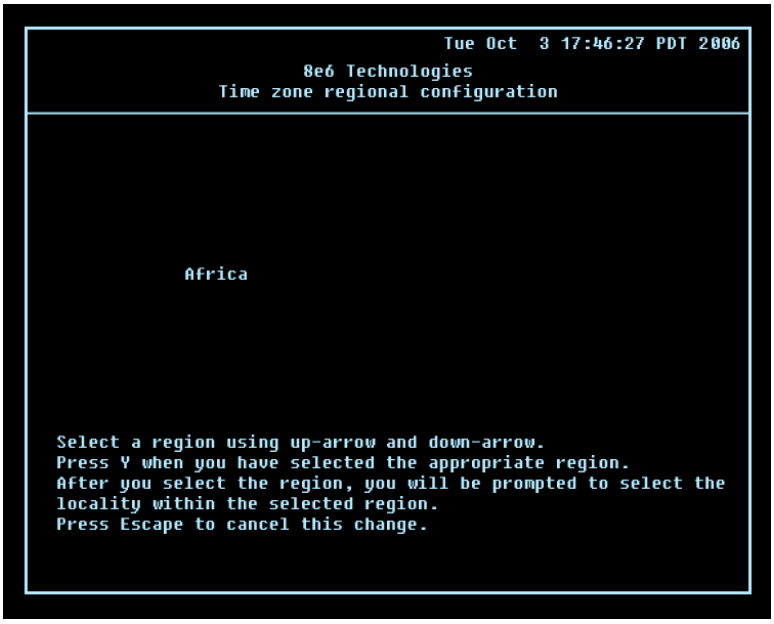


Downloaded from www.Manualslib.com manuals search engine

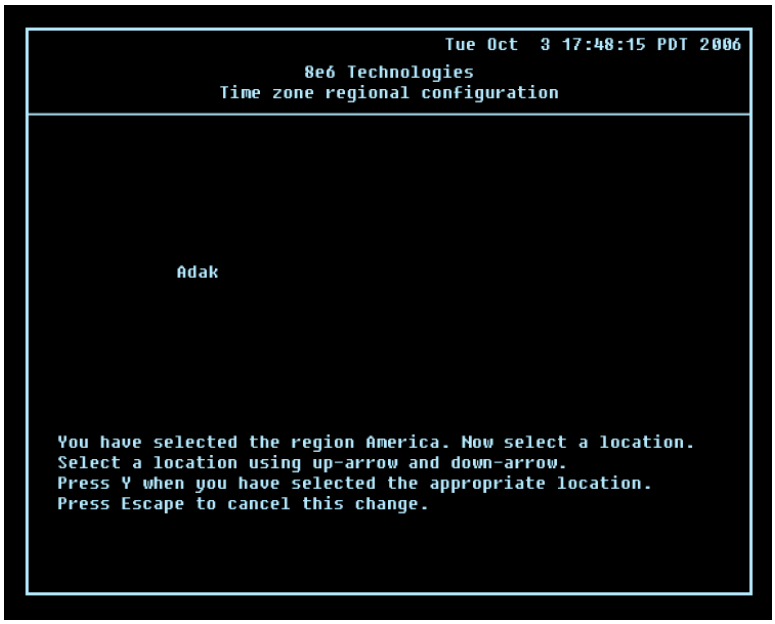
A. At the **Enter host name** field, enter the host name of the server. Press **Enter** to display the confirmation prompt.

B. Press **Y** for “Yes” to confirm and save your entry for the host name, and to go to the Time zone regional configuration screen.

Time zone regional configuration screen


Tue Oct 3 17:46:27 PDT 2006
8e6 Technologies
Time zone regional configuration
Africa
Select a region using up-arrow and down-arrow.
Press Y when you have selected the appropriate region.
After you select the region, you will be prompted to select the locality within the selected region.
Press Escape to cancel this change.

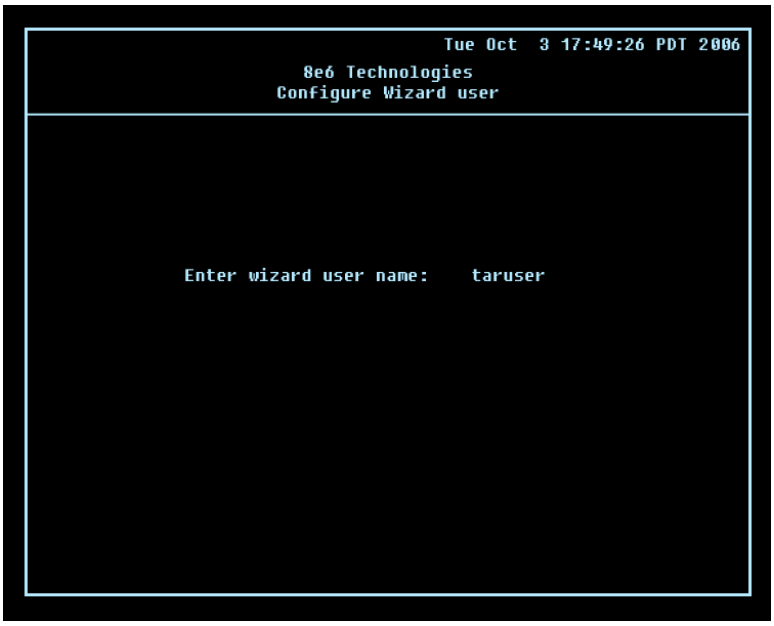
A. Use the up and down arrows in your keyboard to select your region. After selecting your locality, press **Y** for “Yes” to confirm and save your regional selection, and to go to the next screen:


Tue Oct 3 17:48:15 PDT 2006
8e6 Technologies
Time zone regional configuration
Adak
You have selected the region America. Now select a location.
Select a location using up-arrow and down-arrow.
Press Y when you have selected the appropriate location.
Press Escape to cancel this change.

Downloaded from www.Manualslib.com manuals search engine

B. Use the up and down arrows in your keyboard to select your region. After selecting your locality, press **Y** for “Yes” to confirm and save your regional selection, and to go to the Configure Wizard user screen.

Configure Wizard user screen



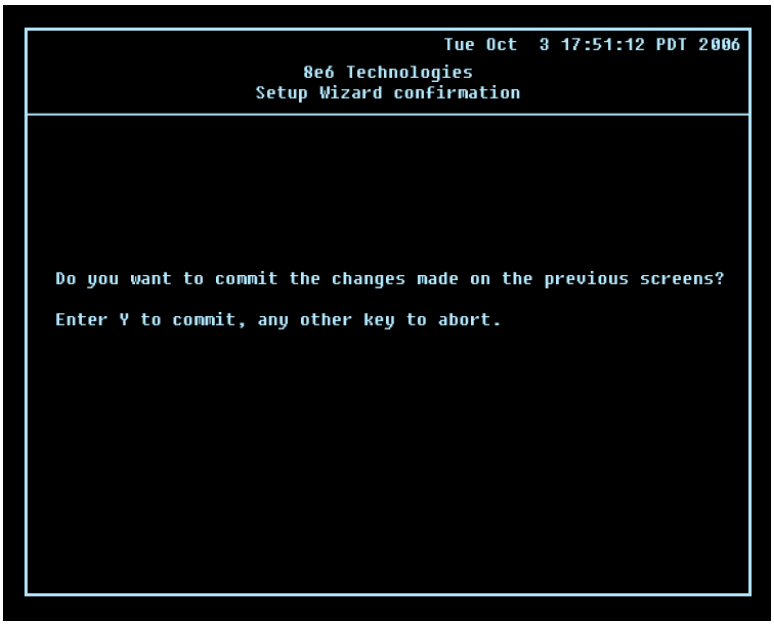
A. At the **Enter wizard user name** field, enter the username that will be used to access the setup wizard in the Threat Analysis Reporter interface. Press **Enter** to display the confirmation prompt.

B. Press **Y** for “Yes” to confirm and save your entry and to go to the next screen.

Downloaded from www.Manualslib.com manuals search engine

C. At the **Enter wizard password** field, enter the password that will be used to access the setup wizard in the Threat Analysis Reporter interface. Press **Y** for “Yes” to confirm and save your entry and to go to the Setup Wizard Confirmation screen.

Setup Wizard Confirmation screen


Tue Oct 3 17:51:12 PDT 2006
8e6 Technologies
Setup Wizard confirmation
Do you want to commit the changes made on the previous screens?
Enter Y to commit, any other key to abort.

Press **Y** for “Yes” to save all your wizard entries and to return to the Administration menu.

NOTE: *When saving your entries, there may be a 4-10 second delay before the Administration menu displays.*

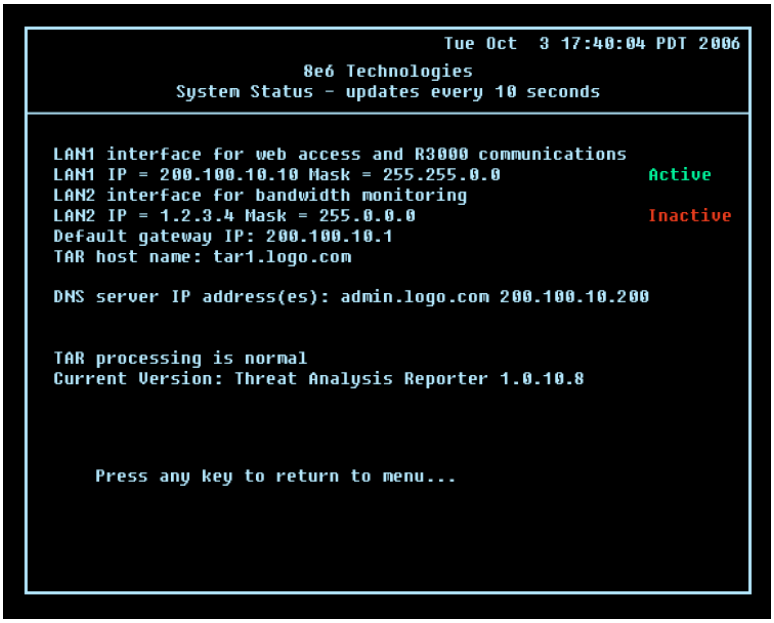
Administration menu

After making all entries using the step-by-step initial setup process, you will return to the Administration menu. Press **X** to return to the System Configuration screen. Or, to verify the status of the Threat Analysis Reporter and review the entries you made using the wizard, press **1** to view the System Status screen.

NOTE: *Changing your password using option C, “Change administration password”, will change the password for the console menu but not the Threat Analysis Reporter console login screen.*

Downloaded from www.Manualslib.com manuals search engine

System Status Screen


Tue Oct 3 17:40:04 PDT 2006
8e6 Technologies
System Status - updates every 10 seconds
LAN1 interface for web access and R3000 communications
LAN1 IP = 200.100.10.10 Mask = 255.255.0.0
Active
LAN2 interface for bandwidth monitoring
LAN2 IP = 1.2.3.4 Mask = 255.0.0.0
Inactive
Default gateway IP: 200.100.10.1
TAR host name: tar1.logo.com
DNS server IP address(es): admin.logo.com 200.100.10.200
TAR processing is normal
Current Version: Threat Analysis Reporter 1.0.10.8
Press any key to return to menu...

The System Status screen contains the following information:

- **LAN1 (eth0) interface for web access and R3000 communications: LAN1 (eth0) IP** address and **netmask** specified in screen 3 (Configure Network Interface), and current status ("Active" or "Inactive")
- **LAN2 (eth1) interface for bandwidth monitoring: LAN2 (eth1) IP** address and **netmask** specified in screen 4 (Configure Network Interface), and current status ("Active" or "Inactive")
- **Default gateway IP** address specified in screen 5 (Configure default gateway)
- **Configure host name** specified in screen 7 (Configure Host Name)
- **DNS server IP address(es)** specified in screen 6 (Configure Domain Name Servers)
- Current status of the Threat Analysis Reporter
- Current Version of the Threat Analysis Reporter software

NOTE: *Modifications can be made at any time by returning to the specific screen of the wizard.*

Log Off, Disconnect the Peripherals

A. After completing the wizard setup procedures, return to the System Configuration screen and press **9** to log out.

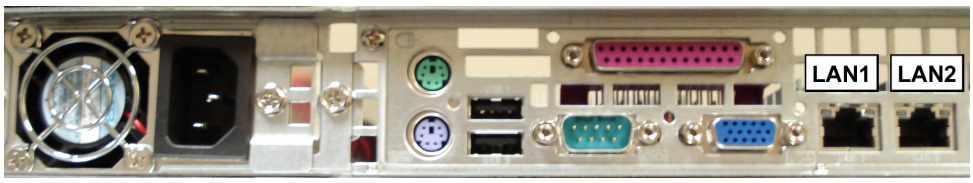
B. Disconnect the peripherals from the Threat Analysis Reporter.

Downloaded from www.Manualslib.com manuals search engine

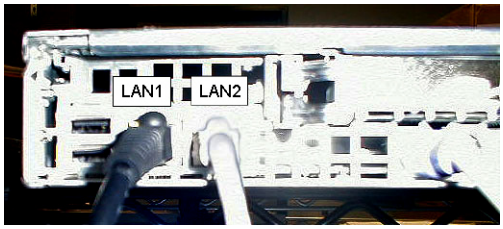
Step 2: Physically Connect the Unit to the Network

After performing initial setup procedures for the Threat Analysis Reporter, the unit should be physically connected to the network. This step requires a standard CAT-5E cable to connect the unit to the network. An additional CAT-5E cable is required if the Ethernet Tap unit will be installed for bandwidth monitoring.

A. Plug one end of a standard CAT-5E cable into the Threat Analysis Reporter's LAN 1 port, the port on the left.



Rear of the "S" and "MSA" chassis



Rear of the "H" chassis

B. Plug the other end of the CAT-5E cable into an open port on the network switch.

Bandwidth Management

If you choose to install the Ethernet Tap for bandwidth monitoring, you will need to connect it to the Threat Analysis Reporter at this point. Refer to Appendix A at the end of this document for instructions on how to connect the Ethernet Tap unit.

Downloaded from www.Manualslib.com manuals search engine

Step 3: Wizard Setup Procedures

For this step, you will need your network administrator to provide you the following information:

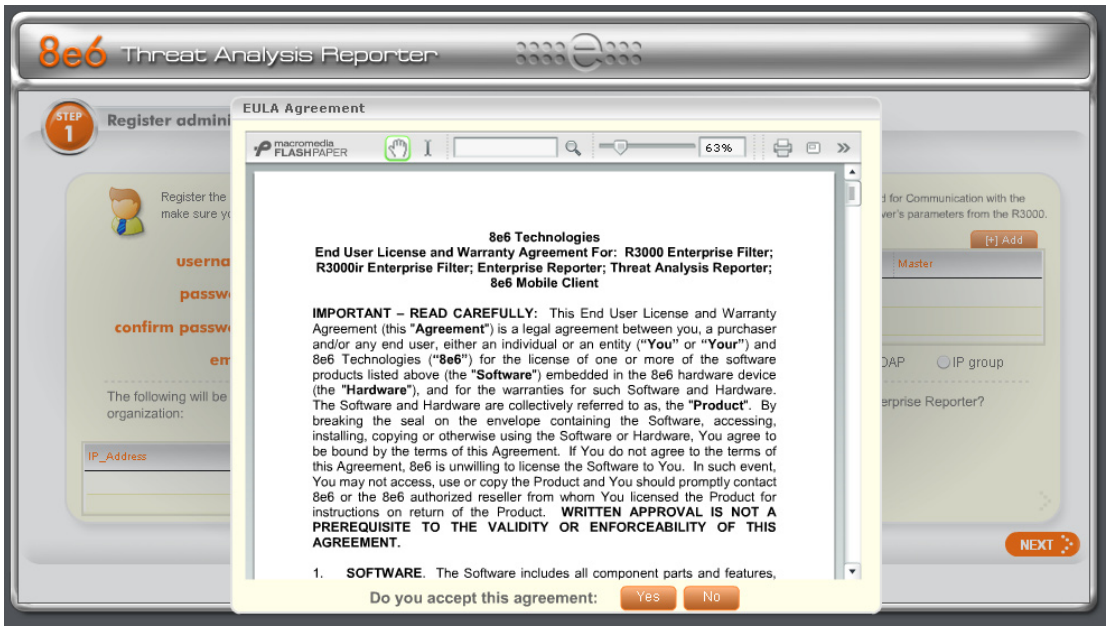
- IP range and netmask of machines on the network the Threat Analysis Reporter server will be monitoring
- R3000 IP address, port number to be used between the R3000 and Threat Analysis Reporter, and type of authentication method to be used (IP group or LDAP)
- 8e6 Enterprise Reporter server IP address and server name, if an ER unit is connected to the R3000

Access the Threat Analysis Reporter Administrator Console

A. Launch Internet Explorer.

B. In the address field, type in **http://x.x.x.x:8080/8e6tar/wizard.html** (in which "x.x.x.x" represents the eth0 IP address entered in the Connect Network Interface screen of the Step-by-Step Initial Setup Procedures). In our example, this entry would be: ***http://200.100.10.10:8080/8e6tar/wizard.html***.

C. Click **Go** to open the Threat Analysis Reporter interface and the EULA Agreement dialog box:


8e6 Threat Analysis Reporter
EULA Agreement
63%
8e6 Technologies
End User License and Warranty Agreement For: R3000 Enterprise Filter; R3000ir Enterprise Filter; Enterprise Reporter; Threat Analysis Reporter; 8e6 Mobile Client
IMPORTANT – READ CAREFULLY: This End User License and Warranty Agreement (this "Agreement") is a legal agreement between you, a purchaser and/or any end user, either an individual or an entity ("You" or "Your") and 8e6 Technologies ("8e6") for the license of one or more of the software products listed above (the "Software") embedded in the 8e6 hardware device (the "Hardware"), and for the warranties for such Software and Hardware. The Software and Hardware are collectively referred to as, the "Product". By breaking the seal on the envelope containing the Software, accessing, installing, copying or otherwise using the Software or Hardware, You agree to be bound by the terms of this Agreement. If You do not agree to the terms of this Agreement, 8e6 is unwilling to license the Software to You. In such event, You may not access, use or copy the Product and You should promptly contact 8e6 or the 8e6 authorized reseller from whom You licensed the Product for instructions on return of the Product. WRITTEN APPROVAL IS NOT A PREREQUISITE TO THE VALIDITY OR ENFORCEABILITY OF THIS AGREEMENT.
1. SOFTWARE. The Software includes all component parts and features,
Do you accept this agreement:
Yes
No
NEXT

Downloaded from www.Manualslib.com manuals search engine

D. After reading the End User License Agreement, you have the option to do either of the following:

- Click **No** to close both the EULA Agreement dialog box and the Threat Analysis Reporter interface. You will not be able to enable the Threat Analysis Reporter for use in your environment.
- Click **Yes** to close the EULA Agreement dialog box and to open the Login dialog box:

Proceed to the next sub-section: Log in to the Threat Analysis Reporter Administrator Console.

Log in to the Threat Analysis Reporter Administrator Console

A. In the **Username** field of the Login dialog box, type in the username specified in the Configure Wizard user screen of the Step-by-Step Initial Setup Procedures. In our example, this entry would be: ***taruser***.

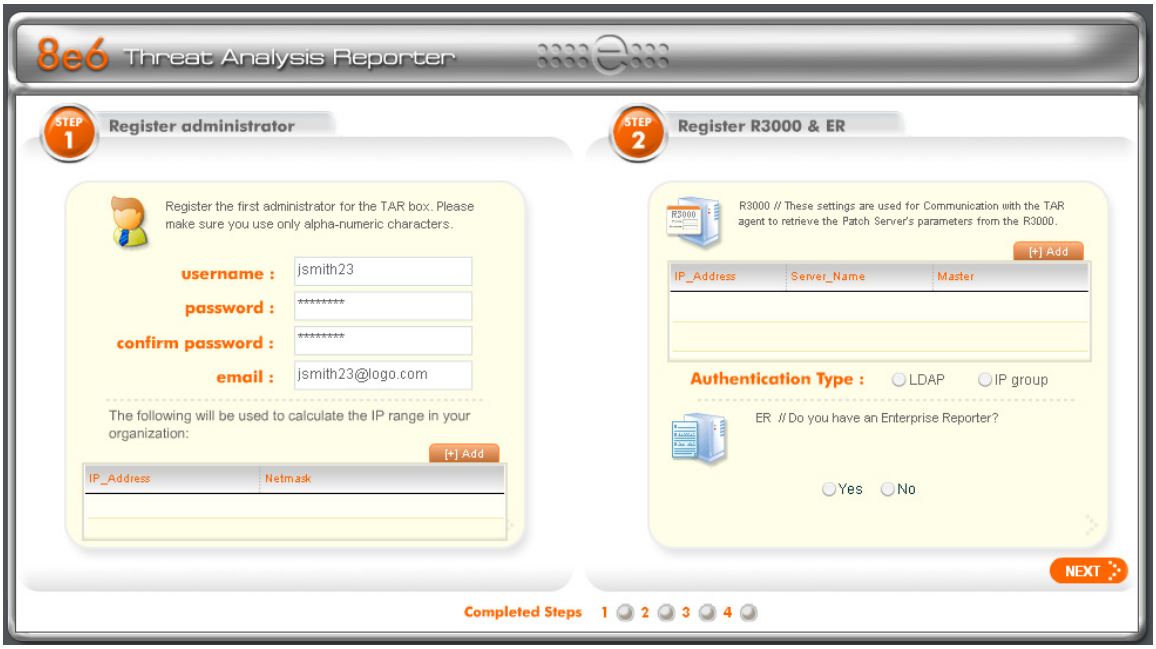
B. In the **Password** field, type in the password specified in the Configure Wizard user screen of the Step-by-Step Initial Setup Procedures.

C. Click **LOGIN** to close the login dialog box and to go to Step 1 of wizard setup procedures in the Threat Analysis Reporter Administrator console (see Step 1: Register administrator).

Downloaded from www.Manualslib.com manuals search engine

Step 1: Register administrator

Step 1 is performed in the left side of the first screen of the wizard:



A. Enter the **username** the global administrator will use when logging into the Threat Analysis Reporter Administrator console. The global administrator has the highest level of permissions in the Threat Analysis Reporter interface.

B. Enter the **password** to be used with that username, and enter the same password again in the **confirm password** field.

C. Enter the **email** address of the global administrator, who will be notified via email when gauges reach their specified upper threshold limits.

Downloaded from www.Manualslib.com manuals search engine

D. Click the [+] Add tab beow to open the IP Range Information dialog box:

E. Enter the **IP address** range for the bandwidth the Threat Analysis Reporter will monitor.

F. Enter the **Netmask** for the IP range to be monitored, using the dotted decimals notation format.

G. Click **OK** to close the dialog box and to display your entries in the list box:

Downloaded from www.Manualslib.com manuals search engine

NOTE: *Additional IP address ranges can be included by clicking the [+] Add tab again and making the entries described in steps E through G above.*

To modify an IP address range, double-click the entry in the list box to highlight it and to display the [-] Remove tab to the left of the [+] Add tab:

- To modify the entries made for the IP address range, click the [+] Add tab to re-open the IP Range Information dialog box and edit information, as necessary. Click **OK** to close the dialog box and to display the modified information in the list box.

- To remove the entry for the IP address range from the list box, click the [-] Remove tab. Click the [+] Add tab to open the IP Range Information dialog box and make new entries for the IP address range.

Downloaded from www.Manualslib.com manuals search engine

Step 2: Register R3000 & ER

Step 2 is performed in the right side of the first screen of the wizard.

R3000:

Specify information for the R3000 to be used with the Threat Analysis Reporter:

A. Click the [+] Add tab above the R3000 list box to open the R3000 Information dialog box:

B. Enter the **IP address** of the R3000 server to be used with the Threat Analysis Reporter. In our example, this is: ***200.100.160.74***, which is the Ethernet 1 IP address of the R3000 server.

C. Enter the **Server Name** of the R3000 to be used with the Threat Analysis Reporter, which is any name you wish to associate with that R3000. In our example, this is: ***R3000LOGO***.

D. Respond to the question “Is this your Master R3000?” by clicking the “Yes” checkbox, if this R3000 will be designated the master R3000 to be associated with the Threat Analysis Reporter. Otherwise, leave the checkbox blank.

Downloaded from www.Manualslib.com manuals search engine

E. Click **OK** to close the dialog box and to display your entries in the list box:

8e6 Threat Analysis Reporter
STEP 1
Register administrator
Register the first administrator for the TAR box. Please make sure you use only alpha-numeric characters.
username : jsmith23
password : ********
confirm password : ********
email : jsmith23@logo.com
The following will be used to calculate the IP range in your organization:
[+] Add
IP_Address Netmask
200.100.10.10 255.255.255.248
STEP 2
Register R3000 & ER
R3000 // These settings are used for Communication with the TAR agent to retrieve the Patch Server's parameters from the R3000.
[+] Add
IP_Address Server_Name Master
200.100.160.74 R3000LOGO Master
Authentication Type : LDAP IP group
ER // Do you have an Enterprise Reporter?
Yes No
NEXT
Completed Steps 1 2 3 4

NOTE: *Additional R3000 servers can be included by clicking the [+] Add tab again and making the entries described in steps A through E above.*

To modify an R3000 entry, double-click the R3000 entry in the list box to highlight it and to display the Set as Master tab and the [-] Remove tab to the left of the [+] Add tab:

8e6 Threat Analysis Reporter
STEP 1
Register administrator
Register the first administrator for the TAR box. Please make sure you use only alpha-numeric characters.
username : jsmith23
password : ********
confirm password : ********
email : jsmith23@logo.com
The following will be used to calculate the IP range in your organization:
[+] Add
IP_Address Netmask
200.100.10.10 255.255.255.248
STEP 2
Register R3000 & ER
R3000 // These settings are used for Communication with the TAR agent to retrieve the Patch Server's parameters from the R3000.
Set as Master [-] Remove [+] Add
IP_Address Server_Name Master
200.100.160.74 R3000LOGO Master
200.100.160.77 R3000LOGO2
Authentication Type : LDAP IP group
ER // Do you have an Enterprise Reporter?
Yes No
NEXT
Completed Steps 1 2 3 4

Downloaded from www.Manualslib.com manuals search engine

- To modify the IP address and Server Name for the R3000 server, click the [+] Add tab to re-open the R3000 Information dialog box, and edit information as necessary. Click **OK** to close the dialog box and to display the modified information in the list box.

- To designate an R3000 as the Master R3000 server, click the entry for the R3000 server in the list box to highlight it, and then click the Set as Master tab to display “Master” in the Master column for that entry in the list box.

- To remove the entry for the R3000 server from the list box, click the [-] Remove tab.

F. Specify the **User Authentication method** to be used for monitoring activity on the Threat Analysis Reporter server: “LDAP” or “IP group”:

ER:

Respond to the question “Do you have an Enterprise Reporter?” by clicking the radio button corresponding to either “Yes” or “No”.

- If “No” was selected, click **NEXT >** at the bottom right of the screen to go to Step 3.

- If “Yes” was selected, the IP address and Server Name fields display in place of the radio buttons. The < Back button displays above the Server Name field.

Downloaded from www.Manualslib.com manuals search engine

*NOTE: To change your answer from "Yes" to "No," click the **< Back** button to re-display the question "Do you have an Enterprise Reporter?"*

A. Enter the **IP address** of the ER server to be used with the Threat Analysis Reporter. In our example, this is: ***200.10.101.76***.

B. Enter the **Server Name** of the ER server to be used with the Threat Analysis Reporter. In our example, this is: ***er4logo***.

C. Click **NEXT >** at the bottom right of the screen to go to Step 3.

*NOTE: Upon clicking **NEXT >** the wizard will verify whether the settings made in Step 1 and Step 2 are correct. If there is an error in any entry made, an orange asterisk flashes beside the field in which the error was made. Correct the error and click **NEXT >** again to go to Step 3.*

Downloaded from www.Manualslib.com manuals search engine

Step 3: Register Gauges

Step 3 requires you to specify settings for default gauges to be monitored by the Threat Analysis Reporter. These gauges will display in the Threat Analysis Reporter interface upon logging into the Administrator console.

*NOTE: Return to Step 1 or Step 2 by clicking the **< BACK** button in the lower left corner of this wizard screen.*

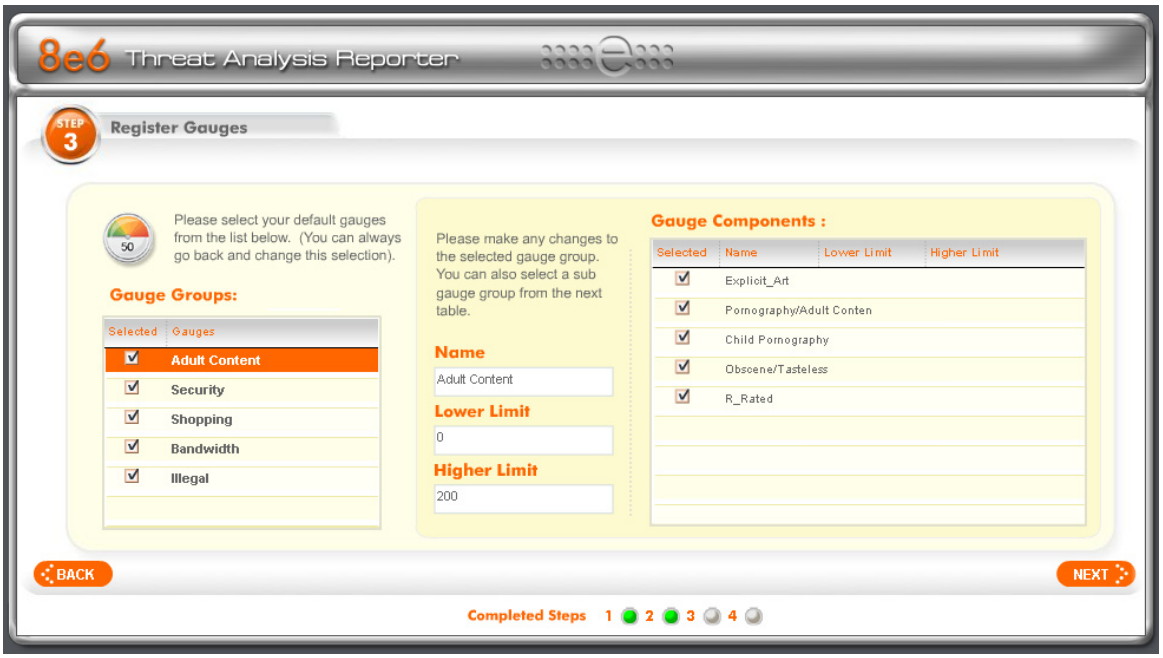
Specify Gauge Groups to be Monitored

By default, all Gauges displayed in this wizard screen (Adult Content, Security, Shopping, Bandwidth, Illegal) are selected for monitoring. To deselect a gauge from the Gauge Groups list, remove the checkmark by clicking the checkbox in the Selected column corresponding to that gauge.

Downloaded from www.Manualslib.com manuals search engine

View, Edit Gauge Components

To view gauge components for a specified gauge, highlight and double-click the gauge name to populate the the fields to the right of the Gauge Groups list box.



The following gauge criteria can be edited:

- **Name**: The displayed gauge name to be used in the interface can be modified by making an entry in this field.
- **Lower Limit**: The default amount (“0” or zero) that will represent the lower end of the gauge can be adjusted to accommodate the type of activity to be monitored on your network.
- **Higher Limit**: The default amount (“200”) that will represent the higher end of the gauge can be adjusted to accommodate the type of activity to be monitored on your network.
- **Gauge Components**: To remove a gauge component, go to the Selected column and click the checkmark in the checkbox corresponding to the component to be removed.

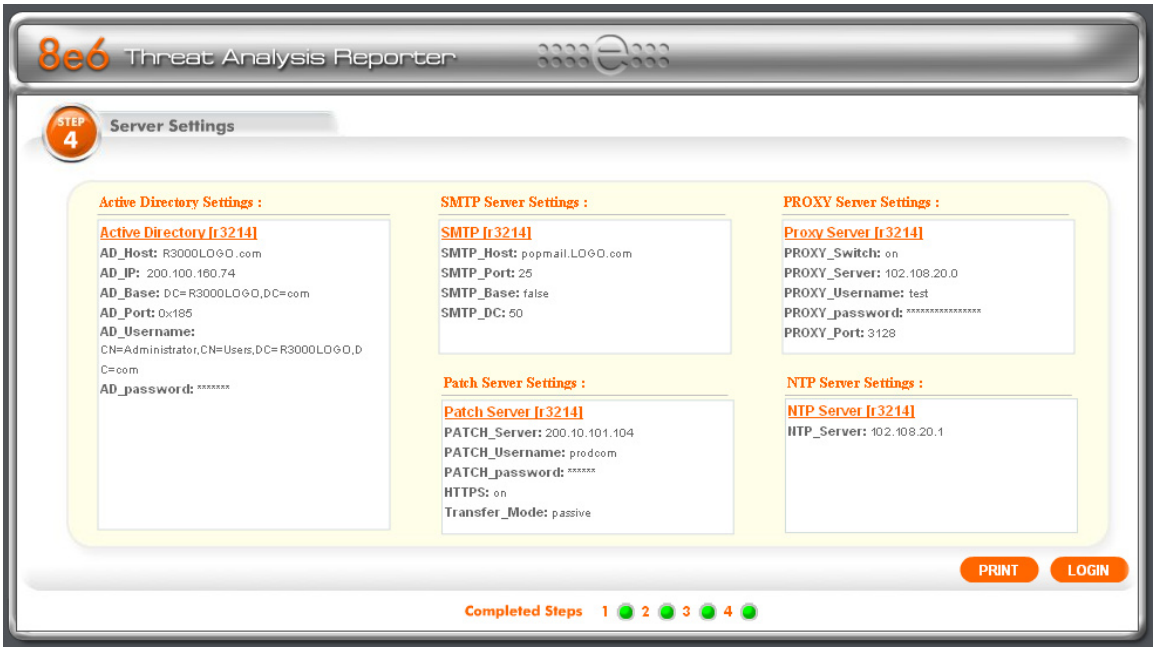
NOTE: *The settings saved in this step can be modified later in the interface.*

Click **NEXT >** at the bottom right of the screen to go to Step 4.

Downloaded from www.Manualslib.com manuals search engine

Step 4: Server Settings

In Step 4, the following R3000 server information displays: Active Directory Settings, SMTP Server Settings, Patch Server Settings, PROXY Server Settings, NTP Server Settings:



*NOTE: Return to Step 3 by clicking the **< BACK** button in the lower left corner of this wizard screen.*

After reviewing the information in this screen, the following actions can now be performed:

- To print this information, click the **Print** button.
- To save all settings entered during the wizard process, click **Save**. After your information is saved, the login dialog box of the Threat Analysis Reporter interface displays, and you can begin using the application.

NOTE: To shut down the Threat Analysis Reporter server, press the power button on the front of the unit to turn off the machine.

Downloaded from www.Manualslib.com manuals search engine

CONCLUSION

Congratulations; you have completed the Threat Analysis Reporter quick start procedures. Now that the Threat Analysis Reporter is running on your network, the next step is to set up user groups or administrator groups. You will set up and configure gauges thereafter.

Obtain the latest Threat Analysis Reporter User Guide from our Web site at **http://www.8e6.com/docs/tar_ug.pdf**.

Downloaded from www.Manualslib.com manuals search engine

SPECIFICATIONS

Physical Specifications

Specification	"S" Value	"H" Value	"MSA" Value
Height	1.7" (43mm)	1.7" (43mm)	1.7" (43mm)
Width	16.8" (426mm)	17.2" (438mm)	16.8" (426mm)
Depth	22.6" (574mm)	26.8" (681mm)	14.0" (356mm)
Front clearance	2 inches (76mm)	2 inches (76mm)	2 inches (76mm)
Side clearance	1 inch (25mm)	1 inch (25mm)	1 inch (25mm)
Rear clearance	3.6 inches (92mm)	3.6 inches (92mm)	3.6 inches (92mm)
Weight	19.5 lbs (8.85 kg)	43.0 lbs (19.5 kg)	11 lbs, 5 oz (5.13 kg)

Internal Product Specifications

Specification	"S" Value	"H" Value	"MSA" Value
CPU	2.0GHz P4 CPU	2x3.6GHz Xeon CPU	2.0GHz Celeron CPU
Memory	3GB PC4200 / DDR2-533 Dual Channel ECC RAM	3GB PC2700 / DDR-333 ECC SDRAM	3GB PC2700 / DDR-333 Dual Channel RAM
Hard drive capacity	1x250GB HDD	2x250GB HDD	1x250GB HDD
Connectivity	10/100/1000	10/100/1000	10/100/1000 10/100/1000

Downloaded from www.Manualslib.com manuals search engine

Hardware Component Specifications

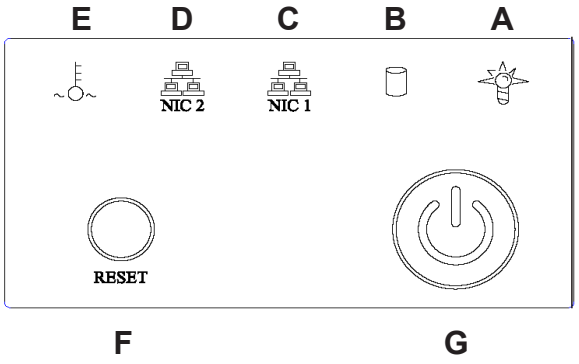
Specification	"S" Value	"H" Value	"MSA" Value
Operating temperature range	10° C ~ 35° C (50° F ~ 95° F)	10° C ~ 35° C (50° F ~ 95° F)	10° C ~ 35° C (50° F ~ 95° F)
Storage temperature range	-40° C ~ +60° C (-40° F ~ 158° F)	-40° C ~ +60° C (-40° F ~ 158° F)	-40° C ~ +70° C (-40° F ~ 158° F)
Operating humidity range	8 ~ 90% non-condensing	8 ~ 90% non-condensing	8 ~ 90% non-condensing
Storage humidity range	5 ~ 95% non-condensing	5 ~ 95% non-condensing	5 ~ 95% non-condensing
Power supply	260W AC power supply [24-pin, (4-pin = 12V)]	560W Hot-swap redundant AC power supply with PFC [24-pin, (8-pin = 12V)]	Thermal control 260W AC power supply with PFC [24-pin, (4-pin = 12V)]
Rated AC input voltage	100 ~ 240V, 50/60Hz, 5-3 Amp	100 ~ 240V, 60-50Hz, 10-5 Amp per power supply module (two modules included in the chassis)	100 ~ 240V, 60-50Hz, 5-3 Amp
Rated input frequency	50 ~ 60 Hz	50 ~ 60 Hz	50 ~ 60 Hz
Rated input current	5A MAX	10A (115V) to 5A (230V)	5A MAX
Rated output power	260W	560W	260W
Maximum rated BTU	1370 BTUs/Hr	N/A (see specs below)	N/A (see specs below)
Nominal DC output: +3.3V	15.0A	21.0A	15.0A
Nominal DC output: +5V	25.0A	30.0A	25.0A
Nominal DC output: +12V	18.0A	42.0A	18.0A
Nominal DC output: -12V	1.0A	1.0A	1.0A
Nominal DC output: +5V standby	2.0A	4.0A	2.0A
Regulatory (power supply)	Power Supply Safety / EMC USA - UL listed, FCC Canada - CUL listed Germany - TUV Certified Europe/CE Mark EN 60950/IEC 60950-Compliant	EN 60950/IEC 60950-Compliant UL Listed (USA) CUL Listed (Canada) TUV Certified (Germany)	USA - UL listed, FCC Canada - CUL listed Germany - TUV Certified Europe/CE Mark EN 60950/IEC 60950-Compliant

Downloaded from www.Manualslib.com manuals search engine

“S” and “MSA” Front Panel LED Indicators, Buttons

Diagrams and Descriptions

On “S” and “MSA” units, LED indicators and buttons display on the front panel to the right:



LED indicators alert you to the status of a feature on the unit while buttons let you perform a function on the unit.

LED Indicators and Buttons

LED Indicator Key

A. Power
B. HDD Activity
C. LAN 1
D. LAN 2
E. Overheat

Button Key

F. Reset
G. Power

LED Indicator	Color	Condition	Description
Power	Green	On	System On
		Off	System Off
HDD	Amber	Blinking	HDD Activity
		Off	No HDD Activity
LAN 1 & LAN 2	Green	On	Link Connected
		Blinking	LAN Activity
		Off	Disconnected
Overheat	Red	On	System Overheated
		Off	System Normal

Downloaded from www.Manualslib.com manuals search engine

APPENDIX: OPTIONAL ETHERNET TAP INSTALLATION

This appendix pertains to the optional installation of the Ethernet Tap unit for bandwidth monitoring.

Preliminary Setup Procedures

Unpack the Ethernet Tap Unit from the Box

Open the NetOptics Ethernet Tap box and verify that all accessories are included. Save all packing materials in the event that the unit needs to be returned to 8e6 Technologies.

The NetOptics box should contain the following items:

- 1 NetOptics 10/100BaseT Tap
- 2 Power Supply units
- 2 AC Power cords
- 2 Crossover cables
- 2 Straight through cables
- 1 Installation Guide

Other Required Installation Items

In addition to the contents of the NetOptics box, you will need the following item to install the Ethernet Tap unit:

- 1 Standard CAT-5E cable

Inspect the box for damage. If the contents appear damaged, file a damage claim with the carrier immediately.

Downloaded from www.Manualslib.com manuals search engine

Install the Ethernet Tap Unit

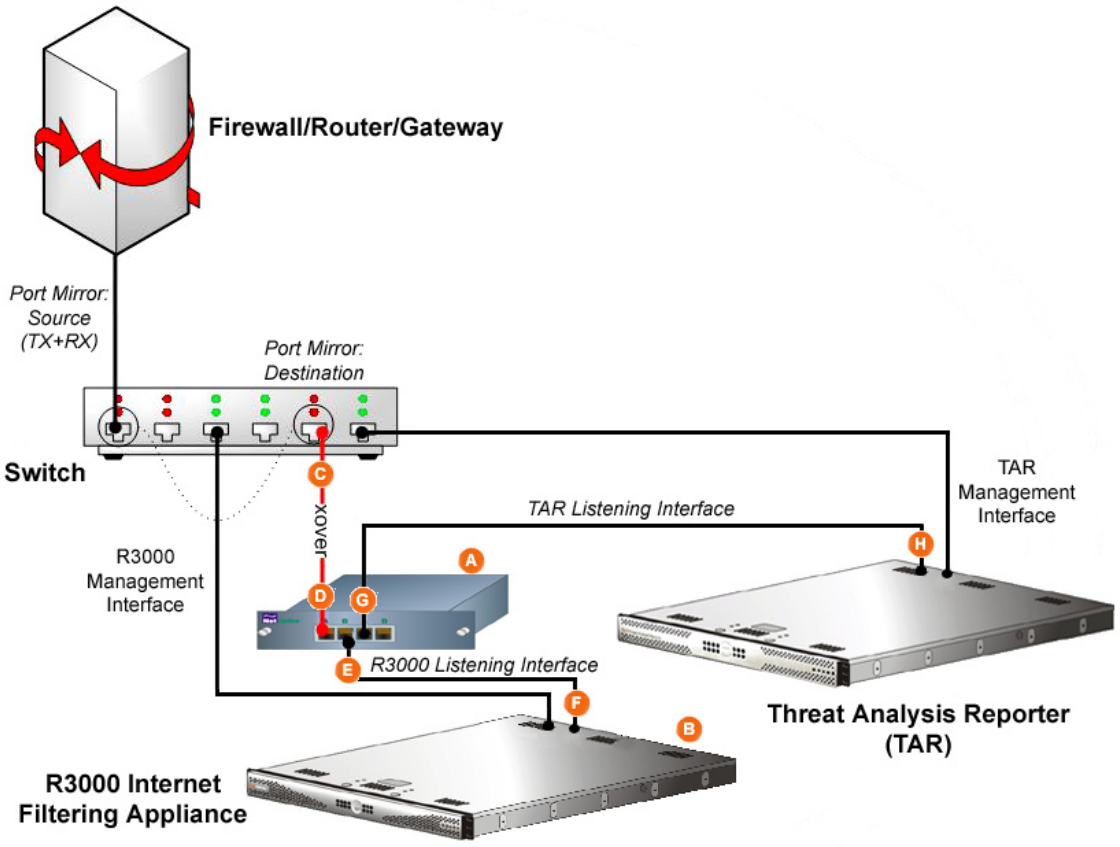


Diagram showing TAR Ethernet Tap installation on the network

This step is a continuation from Step 2: Physically Connect the Unit to the Network. The procedures outlined in this step require the use of a CAT-5E cable.

A. Provide power to the Ethernet Tap by connecting both power cords from the unit to the power source.

AC power in rear panel of NetOptics 10/100BaseT Tap

B. If a designated master R3000 (to be used with the Threat Analysis Reporter) is already installed on the network, disconnect the cable that connects this R3000 to the switch.

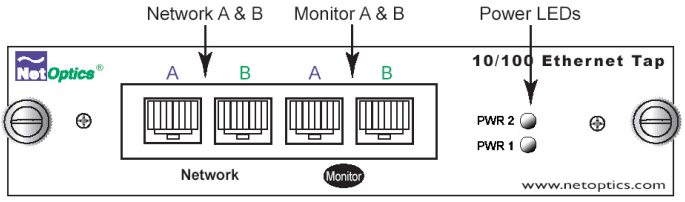
   If the designated R3000 has not yet been installed, disregard this sub-step and proceed to sub-step C.

Downloaded from www.Manualslib.com manuals search engine

C. Using a crossover cable, connect one end to the Switch's port configured to be the destination port of the Port Mirror.

   If adding a Threat Analysis Reporter to an existing installation, this port would be the port that was originally occupied by the listening interface of the R3000.

D. Connect the other end of the crossover cable to the Ethernet Tap's Network A port.



Ports in front panel of NetOptics 10/100BaseT Tap

E. Using a straight through cable, connect one end to the Ethernet Tap's Network B port.

F. Connect the other end of the straight through cable to the R3000's listening interface.

G. Using the second straight through cable, connect one end to the Ethernet Tap's Monitor A port.

H. Connect the other end of the second straight through cable to the Threat Analysis Reporter's listening interface.

Proceed to Step 3: Wizard Setup Procedures of the Threat Analysis Reporter installation instructions.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

8e6 Corporate Headquarters (USA):
828 West Taft Avenue Orange, CA 92865-4232 • Tel: 714.282.6111 or 888.786.7999
Fax: 714.282.6116 (Sales/Technical Support) • 714.282.6117 (General Office)

Satellite Office:
8e6 Taiwan: RM B2, 13F, No. 49, Sec. 3, Minsheng E. Rd., Taipei 104, Taiwan, R.O.C.
Tel: 886-2-2501-5285 • Fax: 886-2-2501-5316

Downloaded from www.Manualslib.com manuals search engine